UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

SNAP-ON BUSINESS SOLUTIONS, INC. Plaintiff, v. O'NEIL & ASSOCIATES, INC. Defendant.	)	CASE NO. 5:09-CV-01547-JG JUDGE JAMES S. GWIN

DECLARATION OF GREGORY D. FEEZEL IN SUPPORT OF SNAP-ON'S OPPOSITION TO O'NEIL'S MOTION FOR SUMMARY JUDGMENT

I, Gregory D. Feezel, hereby declare as follows:

1. I am over twenty-one (21) years of age and, except as may be qualified below, I have personal knowledge of the matters reflected herein and am competent to testify thereto.

2. I am the Director of Security and IT Risk Management for Plaintiff Snap-on Business Solutions, Inc. ("Snap-on"). As such, I have personal knowledge of the websites on which Snap-on hosted data for Mitsubishi Caterpillar Forklift ("MCF") and its related entities, as well as the Snap-on computer servers which host those websites.

3. I also have personal knowledge of the security measures taken by Snap-on to protect its servers and the websites and data they hold, as well as the traffic on the various Snap-on-hosted websites.

4. In order to access any of the MCF websites, users must enter a log-in and password.

5. The use of a single log-in and password to access Snap-on's servers multiple times, especially if used on the MCFA, MCFE, and MCFS systems, would have alerted Snap-on that someone was accessing the servers without authorization.

6. Had O'Neil & Associates, Inc. ("O'Neil") run its data scraping tool on the Snap-on servers during peak times in the day when the Snap-on servers experienced heavy traffic, this would have caused additional drag and delay on the servers.

7. Thus, if the data scraping tool had been run during peak hours of operation of the Snap-on servers, Snap-on would have been more likely to detect the data scraping tool because the slow performance of the websites would have led Snap-on to conduct an investigation into the cause.

8. In April of 2009, because of the high volume of data being scraped by O'Neil from the Snap-on servers, the Snap-on website on which O'Neil was running its data scraping tool crashed.

9. While investigating the cause of the website crash, we determined that the cause was enormous spikes in website traffic.

10. The website crashed for a second time on May 7, 2009, and Snap-on investigation led to the same conclusion: that the website had crashed due to a spike in traffic on its servers.

11. Through an investigation into the second crash, Snap-on was able to determine that the IP address, which was the source of the traffic spikes and ultimately the crash of the website, was registered to O'Neil.

12. Through a review of the activity records of the MCF websites, I was able to determine that O'Neil's data scraping tool accessed the log-in/password home screens, which

contain links to the respective End User License Agreements, for the following Snap-on websites:

a. mitforkliftserviceandpartsmanuals.com (MCFE);
b. catforkliftserviceandpartsmanuals.com (MCFE);
c. mitmcfs.partsandwarranty.com (MCFS); and
d. catmcfs.partsandwarranty.com (MCFS).

13. Attached as Ex. 25 to *Snap-on's Opposition to O'Neil's Motion for Summary Judgment* is an abstract prepared with the assistance of counsel from true and accurate copies of log files showing O'Neil accessing the login/password home screens containing links to the EULAs. The actual log files contain hundreds of entries showing access by O'Neil, which is the reason an abstract has been prepared. The actual log files can be made available and were provided to O'Neil in discovery. I have reviewed the abstract and hereby verify it was accurately prepared from the log files.

14. The format of each line of the log entries is as follows:

Date recorded
Time recorded
Service name or instance
IP address of website
Web method used (i.e., GET, POST)
Page path/name
Server service port (i.e., 80)
IP of source/client
HTTP user agent (the web browser type the client used)
HTTP response code (i.e., 200 is OK)
Status indicator

The "Service name or instance" field is used to identify which website was accessed as follows:

W3SVC1579944688	mitforkliftserviceandpartsmanuals.com
W3SVC4096216	catforkliftserviceandpartsmanuals.com
W3SVC306804665	mitmcfs.partsandwarranty.com
W3SVC346979470	catmcfs.partsandwarranty.com

15. IP addresses I observed and tracked back to O'Neil's network were: 66.194.184.34; 66.192.117.98; 66.192.117.101; and 66.194.184.35.

16. Before accessing the data contained within the Snap-on websites identified above, O'Neil's data scraping tool logged in – and passed through – the homepage containing the link to the EULAs.

17. O'Neil's data scraping tool also accessed portions of the websites mitliftmanuals.com and catliftmanuals.com (MCFA), although I have not been able to determine whether O'Neil accessed the log-in/password home page of these two websites.

18. Once it was determined that O'Neil was the cause of the website crash, Snap-on used its firewall to block O'Neil's IP address.

19. In June of 2009, Snap-on discovered that O'Neil was running its data scraping tool from a different IP address than the one that Snap-on had previously blocked.

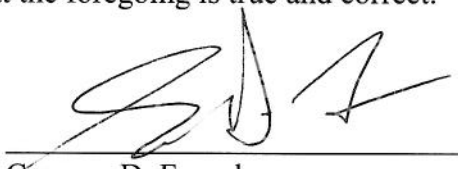
20. The continued running of the scraping tool caused Snap-on further damage by way of customer complaints of slow run-times on the websites, which in turn caused Snap-on to incur additional expenses to diagnose and repair the damage caused by O'Neil.

21. Snap-on was eventually able to block the second IP address used by O'Neil with the Snap-on firewall.

22. From April 2009 through June 2009, Snap-on spent approximately 200 hours diagnosing and repairing the damage caused to Snap-on's servers by O'Neil's scraping activities.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on February 15, 2010



Gregory D. Feezel